(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 317 112 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
04.06.2003 Bulletin 2003/23

(51) Int Cl.[7]: **H04L 29/06**

(21) Application number: **02102644.8**

(22) Date of filing: **26.11.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **29.11.2001 FI 20012339**

(71) Applicant: **Stonesoft Corporation**
00210 Helsinki (FI)

(72) Inventors:
- **Syvänne, Tuomo**
  01450, Vantaa (FI)
- **Jalava, Mika**
  02580, Siuntio (FI)

(74) Representative: **Äkräs, Tapio**
Kolster Oy Ab,
Iso Roobertinkatu 23,
P.O. Box 148
00120 Helsinki (FI)

(54) Handling connections moving between firewalls

(57) A method of handling mobile entities in a firewall, wherein a first mobile entity table comprising identifiers of mobile entities, which are active in a firewall, and a second mobile entity table comprising identifiers of mobile entities, which are active in a predefined set of other firewalls and identifiers of corresponding other firewalls, are maintained (400, 402) in the firewall. A new mobile entity, which is not currently active in the firewall, is detected (404), after which it is found on the basis of the second mobile entity table, if the new mobile entity is currently active in another firewall. If the mobile entity is currently active in another firewall, state information related to the new mobile entity is queried (408) from the another firewall, and stored (410) in the firewall to be used for processing data packets from/to the new mobile entity.

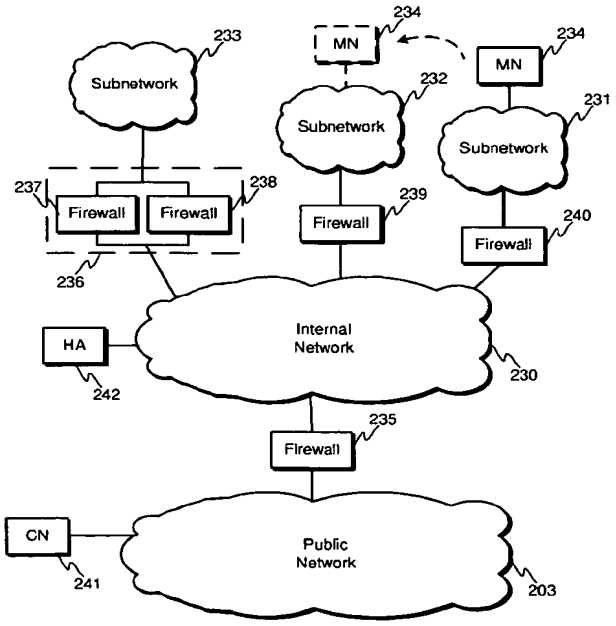

Fig. 2B

EP 1 317 112 A2

Description

Field of the Invention

[0001] The present invention relates to network security and, more particularly, to firewalls or security gateways.

Background of the Invention

[0002] Typically, various organizations protect their internal networks by means of a firewall, which connects the internal network of the organization to public networks and filters and selectively discards the data packets entering and exiting the internal network according to predefined rules. Thus, a firewall is a gateway which operates at the same time as a connector and a separator between the networks in a sense that the firewall keeps track of the traffic that passes through it from one network to another and restricts connections and packets that are defined as unwanted by the administrator of the system. Physically a firewall is a machine with appropriate software to do the tasks assigned to it. It can be a router, a personal computer (PC), or whatever that can be used for such purposes.

[0003] Frequently, the filtering rules of a firewall are expressed as a table or list (rule base) of rules comprising data packet characteristics and related actions. Data packet characteristics are parameter values that are obtained from header field of a data packet and may be e. g. source IP (Internet Protocol) address, destination IP address and service (or protocol) or some other values. The action gives information about how to handle a data packet, which corresponds the data packet characteristics defined in the respective rule (i.e. which matches the rule). This means that for a data packet, which has the header information indicated in a rule, the action indicated in the rule is carried out. In a firewall, the action is typically *deny* or *allow,* which means the data packet is discarded or allowed to proceed, correspondingly.

[0004] The rules of a rule base are examined in certain order until a decision how to process the data packet is reached. The order of the rules in the rule base typically defines the order in which characteristics of a data packet are compared to the rules, that is, the rules are examined one by one from the beginning of the rule base. When a rule, to which the characteristics of a data packet match, is found, the action that is related to that rule is taken and often there is no need to continue examining the rules. However, the action defined in the rule may be *continue,* in which case examining the rule base is continued from the next rule, or *jump*, in which case examining the rule base is continued from the rule specified in the *jump* action. The action of the firewall may be as well *reject,* which is similar to *deny* action. The difference is that *deny* action results in simply discarding the data packet and in *reject* the sender of the data packet is notified of discarding the data packet.

[0005] Figure 1 illustrates as an example a rule base 10, having 5 rules. In each rule, a rule number, source IP address SRC ADDR, destination IP address DST ADDR, service (or protocol) and action are defined. However, this is only an example structure of rules, and also some other data packet characteristics may be defined in the rules. The rule #1 allows HTTP (Hyper-Text Transfer Protocol) data from any address to a server with IP address 172.16.1.10. All other HTTP traffic is denied with rule #2. That is, if HTTP traffic does not match the rule #1, it is denied. Rules #3 and #4 allow FTP (File Transfer Protocol) traffic from network 10.1.1.0 to FTP server at IP address 192.168.1.15 and Telnet connections from network 10.1.1.10 to any address, respectively. The firewall rule bases are commonly designed to prohibit all that is not expressly permitted in the rules. Therefore, the last rule in the rule base is usually designed to deny any data packet. Rule #5 in the rule base 10 is such rule, that is, it denies data packets of related to any service from any source address to any destination address. So, if a data packet does not match any of the first four rules, it matches this last one and is denied.

[0006] In summary, when a data packet is received in the firewall, some of the header field values of the data packet are compared to the rules, which are stored in the firewall, and when a matching rule is found, the action related to the matching rule is taken.

[0007] In a stateful firewall, information about connection history is maintained. In general, a data packet opening a connection is compared to the rules in the rule base, and if the data packet is allowed, a state is created for the opened connection. The state is created by making into a connection state table an entry including information for identifying the connection (e.g. source and destination address, ports and/or protocol) and the state of the connection. Other than data packets opening a connection are then compared to the connection state table and allowed, if a corresponding entry is found and the data packet is in accordance with the state of the connection. At the same time the state of the connection in the connection state table may be updated. If a corresponding entry is not found in the state table, the data packet may be compared to the rules in the rule base and possibly allowed on the basis of rules or simply discarded. Stateful inspection makes processing of data packets belonging to open connections faster than simple packet filtering on the basis of rules. Additionally, state of the connections (the data packets that have already been allowed and possibly their content) can be taken into account in processing data packets, which makes stateful firewall more secure than simple packet filter. Therefore stateful processing is desirable.

[0008] Traditionally, IP (Internet Protocol) address of an entity uniquely identifies the entity's point of attachment to the Internet. Therefore, the entity must be located on the network indicated by its IP address in order to communicate using the IP address. Otherwise, the data packets destined to the entity by using its IP address

would not be deliverable. Mobile IP (Internet Protocol) is a protocol for enabling an entity to change its point of attachment to the Internet without changing the IP address it is using. That is, an entity can use the same IP address even if its location in the network changes. From the network point of view, this means that the path used to deliver the traffic for the entity can change.

[0009] According to mobile IP, each mobile node (or entity) is always identified by its home IP address, regardless of its current point of attachment to the Internet. When the mobile node (MN) is outside its home network and therefore not directly reachable by its home IP address, a care-of address, which provides information about its current point of attachment to the Internet, is assigned the mobile node in addition to the home IP address. The care-of address may be the IP address of a foreign agent (FA) located in the network the mobile node is visiting or it may be a co-located care-of address, which is an address of the network the mobile node is visiting, which is dynamically assigned to the mobile node (e.g. by means of DHCP, Dynamic Host Configuration Protocol). The mobile node registers the care-of address with a home agent (HA) in its home network by sending a Registration Request message (UDP, User Datagram Protocol, data packet to port 434) to which the home agent responds with a Registration Reply message in IPv4, which is the "current" version of Internet Protocol. In IPv6, which is the next generation of Internet Protocol, the registration is done by means of specific Extension Headers, wherein Binding Update and Binding Acknowledgement Destination Options (corresponding to Registration Request and Registration Reply respectively) are transmitted.

[0010] When the mobile node is in its home network, it communicates with other entities by using its home IP address normally. When the mobile node is outside its home network, that is, in a foreign network, other entities still reach the mobile node by using its home IP address. After the home agent has been notified that the mobile node is in a foreign network with a Registration Request message / Binding Update Destination Option giving the mobile nodes current care-of address, the home agent intercepts the data packets destined to the mobile node's home IP address. The home agent then encapsulates these data packets to data packets destined to the mobile node's care-of address (tunnels data packets) for delivery to the mobile node. If the care-of address is the address of the foreign agent, the foreign agent is the endpoint of the tunnel and it decapsulates the data packet and delivers the original data packet to the mobile node. Similarly, if the care-of address is a co-located care-of address, the mobile node is the endpoint of the tunnel and it decapsulates the data packet for obtaining the original data packet. The mobile node sends reply packets directly to the other end. In IPv6, the mobile node sends reply packets by using its care-of address as source address, and attaches its home address to a Home Address Extension Header. In this way the data packets are routed correctly (correct source address) and the other end is able to identify the mobile node by extracting the static home address form the Home Address Extension Header. After this the other end may communicate directly with the mobile node; this is done by using the care-of address of the mobile node as a destination address, but including also mobile node's home address in data packets in a Routing Extension Header.

[0011] The methods of mobile IP are deployed also in General Packet Radio Service (GPRS). GPRS Tunneling Protocol (GTP) is the protocol used between GPRS Support Nodes (GSNs) in the UMTS/GPRS backbone network. It includes both the GTP signaling (GTP-C) and data transfer (GTP-U) procedures. In GPRS, special support nodes called Gateway GPRS Support Nodes (GGSN) and Gateway Serving GPRS Support Nodes (SGSN) are deployed. SGSNs provide the direct access point for GPRS phones, subtending from GGSNs that provide the gateway to SGSNs across mobile networks that the user may visit. The GGSN also is the access point for other packet data networks, such as Internet, and therefore enables communication between "normal" IP networks and GPRS devices. GTP is used to forward packets from GGSN to SGSN to reach a mobile device, dynamically setting up tunnels between GGSN and its home network and allowing the mobile unit to have its home network served beyond the GGSN Internet Gateway. GTP allows the GPRS user to be reachable from data networks, such as Internet, by using the same addressing information irrespective of its point of attachment to the network.

[0012] It is common that there is one firewall protecting the home network of a mobile node, and another firewall protecting a foreign network the mobile node is visiting. These networks may for example subnetworks belonging to the same organisation. Statefull filtering in a firewall uses information about previous packets of a connection for processing other data packets of the connection. In a situation, where statefull firewall starts seeing traffic in the middle of a connection it lacks the necessary information for processing the data packets and therefore discards the data packets and the respective connection fails. This happens when a mobile node moves from one network to another without changing the addressing information it is using. Therefore, information about the state of the connections needs to be shared between firewalls in order to enable connection roaming from one firewall to another.

[0013] In clustered firewalls (multiple parallel firewalls) and high availability solutions the state information is shared between firewalls (synchronization of state information) in order to enable one firewall to continue processing of a connection previously processed by another firewall. In these solutions, the state of each connection currently processed in each relevant firewall is usually synchronized to all other firewalls. This is feasible in a clustered firewall, since any of the cluster

members need to be ready for taking over the connections processed by some other cluster member, and the number of the cluster members is in practice limited to a reasonable number. However, synchronizing all available state information between firewalls does not suit well for handling the location changes of mobile IP users. The distance between firewalls sets some limitations to the amount of information that is feasible to be shared. Additionally, synchronizing all state information would result in sharing unnecessary information as well, since many of the connections handled by the firewalls are from static sources and only some may involve a mobile user.

[0014] Due to these deficiencies, a more suitable method for enabling connection roaming between firewalls is needed.

Summary of the Invention

[0015] An object of the invention is to fulfill the need described above by providing a method for handling mobile entities in firewalls and maintaining information in firewalls.

[0016] The objects of the invention are achieved according to the invention as disclosed in the attached independent claims. Preferred embodiments of the invention are disclosed in the dependent claims. The features described in one dependent claim may be further combined with features described in another dependent claim to produce further embodiments of the invention.

[0017] The idea of the invention is to synchronize high level information about active mobile entities between firewalls, and when a mobile entity moves from a first firewall to a second one, to fetch the accurate state information related to the mobile entity from the first one to the second one to be used in the second one for handling the connections of the mobile entity. Where to fetch the information is known on the basis of the synchronized high level information. Information about all active entities in a firewall do not need to be synchronized, but only information about active mobile entities, which may be reached by static addressing information irrespective of their point of attachment to the network. For such mobile entities, the open connections should not fail due to change of location. Information about which IP address may be used by mobile entities or which IP addresses may not be used by mobile entities may be configured in the firewalls in order to identify mobile entities. In practice, the firewalls among which the information is shared are firewall of one organization, e.g. firewall of one company or firewalls of an operator offering connectivity services to a plurality of customers. It is also possible that all connections, which are conveyed inside a tunnel (that is encapsulated into another data packet), are considered as connections, which are potentially used by mobile entities. Therefore, information about the endpoints of such tunnelled connections may be synchronized by the method according to the invention. Also detecting an IPv6 Extension Header (e.g. Home Address Header or Routing Header) can be used for identifying connections of potentially mobile entities.

[0018] According to the invention a first mobile entity table comprising identifiers of mobile entities, which are active in a firewall, and a second mobile entity table comprising identifiers of mobile entities, which are active in a predefined set of other firewalls and identifiers of corresponding firewalls, are maintained in the firewall. An identifier of a mobile entity may be for example an IP address or a subscriber number. Especially if the connections of the mobile entity are transferred within a tunnel, the identifier may be other than an IP address. When a new mobile entity not currently active in the firewall is detected, it is found on the basis of the second mobile entity table, if the new mobile entity is currently active in another firewall, and if the mobile entity is currently active in another firewall, state information related to the new mobile entity is queried from the another firewall, and the received state information is stored in the firewall to be used for processing data packets from/to the new mobile entity.

[0019] Detecting a new mobile entity may involve detecting a data packet in which the source is the new mobile entity or detecting registration of the new mobile entity. The registration may be detected due to negotiation for a new location or detecting routing protocol traffic. For example, the Session Initiation Protocol (SIP) may indicate that a mobile entity is moving from one firewall's influence to another's. A new entry corresponding to the new mobile entity is added in the first mobile entity table after detecting the new mobile entity.

[0020] The state information related to the mobile entity is history information of the open connections of the mobile entity, which is used in stateful connection processing in a firewall. The state information may include also authentication information or some other information used in processing data packets associated to the entity in question.

[0021] A firewall according to the invention sends the first mobile entity table to a predefined set of other firewalls as a response to a predefined action, such as an indication of a certain time period having elapsed since the first mobile entity table was sent the last time, a change in the content of the first mobile entity table, or receiving a request for the first mobile entity table.

[0022] The firewall receives from at least one other firewall a mobile entity table comprising identifiers of mobile entities which are active in the at least one other firewall. On the basis of the received mobile entity table the firewall updates (deletes, adds or modifies entries) its second mobile entity table and deletes an entry in its first mobile entity table, if a corresponding entry is contained in the received mobile entity table. Receiving an entry of the first mobile entity table in a mobile entity table of some other firewall indicates that the corresponding entity has moved from the firewall to the other firewall and may therefore be deleted from the first mo-

bile entity table of the firewall as unnecessary. The state information associated with the mobile entity are in practice queried from the firewall by the other firewall before deleting the corresponding entry in the first mobile entity table of the firewall. Alternatively, entries of a first mobile entity table may be removed also on the basis of a timer.

[0023] The invention relates as well to a method of maintaining information in a firewall, comprising maintaining a first mobile entity table comprising identifiers of mobile entities which are active in the firewall, sending the first mobile entity table to a predefined set of other firewalls as a response to a predefined action, receiving from at least one other firewall a mobile entity table comprising identifiers of mobile entities which are active in the at least one other firewall, and maintaining a second mobile entity table comprising identifiers of mobile entities which are active in the at least one other firewall and an identifier of the corresponding firewall on the basis of the mobile entity table received from at least one other firewall.

[0024] A firewall according to invention may request from at least one other firewall a mobile entity table comprising identifiers of mobile entities which are active in the at least one other firewall for maintaining the first mobile entity table in the firewall.

[0025] Compared to traditional synchronization of state information used e.g. in clusters, the method according to the invention requires much less information transfer between the firewalls.

[0026] These and other features of the invention, as well as the advantages offered thereby, are described hereinafter with reference to embodiments illustrated in the accompanying drawings.

Brief description of the drawings

[0027]

Figure 1 illustrates an exemplary prior art rule base,
Figures 2A, 2B and 3 are schematic block diagrams of exemplary network configurations wherein the present invention can be applied,
Figure 4A is a flow diagram illustrating operation according to one aspect of the invention,
Figure 4B is a flow diagram illustrating detection of a new mobile entity according to the invention,
Figure 5 is a flow diagram illustrating exemplary methods for triggering sending a mobile entity table to other firewalls, and
Figure 6 is a flow diagram illustrating an exemplary method for handling a received mobile entity table.

Preferred embodiments of the invention

[0028] The present invention can be applied in any stateful network gateway or firewall, which is processing data packets of mobile entities, which may be reached by static addressing information irrespective of their point of attachment to the network. For such mobile entities, the open connections should not fail due to change of location.

[0029] The data connectivity of the mobile entity may be through wireless or fixed line connection. Typically such mobile entities are portable computer devices, such as laptop computers, PDAs, communicators, smart phones, intelligent telecommunication devices, etc. The physical location independence of the mobile entities may be based on mobile IP, GTP or some other protocol. The system providing connectivity to the mobile entity may be but is not limited to LAN (Local Area Network), WLAN (Wireless LAN), GSM (Global System for Mobile communications), GPRS (General Packet Radio Service), or UMTS (Universal Mobile Telecommunications System).

[0030] The invention relates to synchronizing high level information about active mobile entities between firewalls, and when a mobile entity moves from a first firewall to a second one, to fetching the accurate state information related to the mobile entity from the first one to the second one to be used in the second one for handling the connections of the mobile entity. Where to fetch the information is known on the basis of the synchronized high level information.

[0031] Figures 2A, 2B and 3 are schematic block diagrams of exemplary network configurations wherein the present invention can be applied. The configurations are shown only to facilitate the understanding and description of the present invention. The present invention is not intended to be restricted to any particular network configuration. Further, in order to improve clarity, mainly only network elements which are somehow involved with the present invention are shown in Figures 2A, 2B and 3.

[0032] Figure 2A shows a network configuration in connection with mobile IP. A subnetwork 200 is connected to a public network 203 via a firewall system 205. The firewall system contains three parallel firewalls 206, 207 and 208 in order to ensure connectivity through the firewall system. However, in the connection of this invention the structure of the firewall system is not relevant. Another subnetwork 202 is connected to the public network via a firewall 204. A mobile node 201 is connected to the subnetwork 200, which is its home network. A home agent 210 is as well connected to the subnetwork 200. The mobile node communicates with a correspondent node 209 attached to the public network 203. With help of the home agent 210, the mobile node may change its point of attachment to the subnetwork 202 (shown with dashed line in Figure 2A) without breaking its connection with the correspondent node 209. In this case, the connection is first handled with the firewall system 205 and then with the firewall 204. Assuming that the firewalls are stateful firewalls and in order not to break the connection state information needs to be shared between the firewalls 204 and 205. Using the method according to the invention in the firewalls enables this.

However, if the mobile node 201 has ongoing connections within the subnetwork 200 before the change of the location, those connections fail after the move, since the firewall system 205 does not have information about the connections inside the subnetwork 200.

[0033] Figure 2B shows another network configuration in connection with mobile IP. Three subnetworks 231, 232 and 233 are connected to an internal network 230 via firewalls 236 (a cluster containing two parallel firewall devices 236 and 237), 239 and 240. The internal network 230 is connected to public network 203 via a firewall 235. A mobile node 234 is connected to the subnetwork 231 and may change its location to any of the subnetworks 232 and 233 (shown with dashed line in Figure 2B), therefore the firewalls 236, 239 and 240 need to be able to handle moving open connections. The physical location of the mobile node 234 is known to a home agent 242 in the internal network. The mobile node may communicate for example with a correspondent node 241 connected to the public network 203.

[0034] Figure 3 illustrates a schematic block diagram of exemplary network configuration related to GPRS system where the invention may be used. Therein two wireless subnetworks 302 and 318 are connected to a service network 308 via SGSNs 304, 320 and GGSNs 306, 322. SGSNs provide the direct access point for GPRS devices in the subnetworks 302, 318. GGSNs that provide the gateway to SGSNs across mobile networks that the user may visit. The GGSN also is the access point for other packet data networks, such as Internet, and therefore enabling communication between "normal" IP networks and GPRS devices. Data is transferred between SGSNs and GGSNs in tunnels according to GTP (GPRS Tunneling Protocol). Between the SGSN 304 and GGSN 306 there is a firewall 305 filtering the GTP tunnel. Accordingly, there is a firewall 321 between the SGSN 320 and the GGSN 322. The service network 308 is further connected to a public network 314 (such as Internet) via a gateway 312, which may or may not be a firewall device.

[0035] In subnetwork 302 there is connected a GPRS device 300, which may communicate with an entity 310 connected to the service network 308 or with an entity 316 connected to the public network 314. These connections go through the firewall 305. The GPRS device 300 may change its location to the subnetwork 318 (shown with dashed line in Figure 3), which causes that the connections of the GPRS device move to the firewall 321.

[0036] Naturally, the coupling between the different networks in Figures 2A, 2B and 3 may include also routers and Internet service providers (not shown in Figures). As is well known in the art, the internal networks or subnetworks may be, for example, company networks, such as a local area networks (LAN) or a wireless LANs (WLAN) which connect users and resources, such as workstations, servers, printers and the like of the company. Alternatively, the internal networks or subnetworks may consist of connections of individual subscribers such as ADSL subscribers or subscribers of a wireless network such as GSM, GPRS or UMTS network. In this case, the term internal network may not be very descriptive, and instead a term such as a service network could be used.

[0037] The method of the invention may be used for example in any of the firewalls 204, 205, 236, 239, 240, 305, 321 discussed above. As already described above, the firewalls 204, 205, 236, 239, 240, 305, 321 are gateways which operate at the same time as connectors and separators between the networks in a sense that the firewalls keep track of the traffic that passes through them from one network to another and restrict connections and packets that are defined as unwanted by the administrators of the systems. Physically a firewall is a device with appropriate software to do the tasks assigned to it. It can be a router, a personal computer (PC), or whatever that can be used for such purposes.

[0038] Figure 4A is a flow diagram illustrating operation according to one aspect of the invention. In steps 400 and 402, a first mobile entity table comprising identifiers of mobile entities, which are active in a firewall, and a second mobile entity table comprising identifiers of mobile entities, which are active in a predefined set of other firewalls and identifiers of corresponding firewalls, are maintained in the firewall. An identifier of a mobile entity may be for example an IP address or a subscriber number. Especially if the connections of the mobile entity are transferred within a tunnel, the identifier may be other than an IP address. In step 404, a new mobile entity not currently active in the firewall is detected. Then, it is found on the basis of the second mobile entity table, if the new mobile entity is currently active in another firewall (step 406). If the mobile entity is currently active in another firewall, state information related to the new mobile entity is queried in step 408 from the another firewall, and the received state information is stored in the firewall to be used for processing data packets from/to the new mobile entity in step 410. In step 412, a new entry corresponding to the new mobile entity is added in the first mobile entity table. If it is found in step 406 that the mobile entity is currently not active in any other firewall, the process proceeds straight to step 412 for adding a new entry. In this case, it is assumed that the mobile entity is only starting communication and does not have any ongoing connections open.

[0039] The state information related to the mobile entity is history information of the open connections of the mobile entity, which is used in stateful connection processing in a firewall. The state information may include also authentication information or some other information used in processing data packets associated to the entity in question.

[0040] Figure 4B is a flow diagram illustrating detection of a new mobile entity according to the invention. Detecting a new mobile entity may involve detecting a data packet in which the source is the new mobile entity

in step 414 or detecting registration of the new mobile entity in step 416. The registration may be detected due to negotiation for a new location or detecting routing protocol traffic. For example, the Session Initiation Protocol (SIP) may indicate that a mobile entity is moving from one firewall's influence to another's. SIP is an Internet Engineering Task Force (IETF) standard protocol for initiating an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality. Because the SIP supports name mapping and redirection services, it makes it possible for users to initiate and receive communications and services from any location, and for networks to identify the users where ever they are. In relation to Mobile IP, the change of location may be detected from Registration Request / Binding Update messages.

[0041] A firewall according to the invention sends the first mobile entity table to a predefined set of other firewalls as a response to a predefined action. Figure 5 is a flow diagram illustrating exemplary methods for triggering sending a mobile entity table to other firewalls. In step 500 it is checked, if a predefined time period has elapsed since the first mobile entity table was sent the last time. If it has, the first mobile entity table is sent in step 502 to a predefined set of other firewalls. In step 504 it is checked, if the content of the first mobile entity table has changed. If it has, the first mobile entity table is sent in step 502 to a predefined set of other firewalls. This may be done also so that when ever an entry is added, deleted or modified in the first mobile entity table, it is sent to the other firewalls. In step 506 it is checked, if a request for the first mobile entity table is received. If it is, the first mobile entity table is sent in step 502 to a predefined set of other firewalls.

[0042] The other firewalls to which the table is sent are typically firewalls of one organization, e.g. of one network operator administering the services offered to the customers by means of firewalls, which allow only the type of connections for the customers they have subscribed for.

[0043] Figure 6 is a flow diagram illustrating an exemplary method for handling a received mobile entity table. In step 600, a firewall receives from at least one other firewall a mobile entity table comprising identifiers of mobile entities which are active in the at least one other firewall. In step 602, the second mobile entity table in the firewall is updated on the basis of the received mobile entity table. Updating involves deleting, adding and/or modifying entries. In step 604 it is checked if one of the entries in the firewall's first mobile entity table is included in the received mobile entity table. If that is the case, the corresponding entry is deleted in the firewall's first mobile entity table in step 606. If there are no entries of the first mobile entity in the received mobile entity table, only the second mobile entity table needs to be updated.

[0044] Receiving an entry of the first mobile entity table in a mobile entity table of some other firewall indicates that the corresponding entity has moved from the firewall to the other firewall and may therefore be deleted from the first mobile entity table of the firewall as unnecessary. The state information associated with the mobile entity are in practice queried from the firewall by the other firewall before deleting the corresponding entry in the first mobile entity table of the firewall. Alternatively, entries of a first mobile entity table may be removed also on the basis of a timer.

[0045] It must be appreciated that the embodiments described above are given as examples only, while the features described in one example may be combined with features of another example and various modifications can be made within the scope and spirit of the invention as defined in the appended claims.

Claims

1. A method of handling mobile entities in a firewall, **characterized in**

   maintaining (400) a first mobile entity table comprising identifiers of mobile entities which are active in the firewall,

   maintaining (402) a second mobile entity table comprising identifiers of mobile entities which are active in a predefined set of other firewal ls and identifiers of corresponding other firewalls,

   detecting (404) a new mobile entity, which is not currently active in the firewall,

   finding (406) on the basis of the second mobile entity table, if the new mobile entity is currently active in another firewall, and

   if the mobile entity is currently active in another firewall, querying (408), from the another firewall, state information related to the new mobile entity, and storing (410) the state information in the firewall to be used for processing data packets from/to the new mobile entity.

2. A method according to claim 1, further **characterized in**

   adding (412) a new entry in the first mobile entity table after detecting a new mobile entity not currently active in the firewall, the new entry corresponding to the new mobile entity.

3. A method according to any one of preceding claims, further **characterized in**

   sending (502) the first mobile entity table to a predefined set of other firewalls as a response to a predefined action.

4. A method according to claim 3, **characterized in that** the predefined action is an indication of certain time period having elapsed (500) since the first mobile entity table was sent the last time.

5. A method according to claim 3, **characterized in that** the predefined action is changing (504) the content of the first mobile entity table.

6. A method according to claim 3, **characterized in that** the predefined action is receiving (506) a request for the first mobile entity table.

7. A method according to any one of preceding claims, further **characterized in**

receiving (600) from at least one other firewall a mobile entity table comprising identifiers of mobile entities which are active in the at least one other firewall,

updating (602) the second mobile entity table on the basis of the received mobile entity table, and

deleting (606) an entry in the first mobile entity table, if a corresponding entry is contained in the received mobile entity table.

8. A method according to any one of preceding claims, **characterized in that** detecting a new mobile entity comprises

detecting (414) a data packet in which the source is the new mobile entity.

9. A method according to any one of claims 1 to 8, **characterized in that** detecting a new mobile entity comprises

detecting (416) a registration message from the new mobile entity.

10. A method according to any one of preceding claims, **characterized in that** the identifier is an IP address or a subscriber number.

11. A method according to any one of preceding claims, **characterized in that** the state information related to the new mobile entity comprises state of the ongoing connections of the new mobile entity.

12. A method of maintaining information in a firewall, **characterized in**

maintaining (400) a first mobile entity table comprising identifiers of mobile entities which are active in the firewall,

sending (502) the first mobile entity table to a predefined set of other firewalls as a response to a predefined action,

receiving (600) from at least one other firewall a mobile entity table comprising identifiers of mobile entities which are active in the at least one other firewall, and

maintaining (402) a second mobile entity table comprising identifiers of mobile entities which are active in the at least one other firewall and an identifier of the corresponding at least one other firewall on the basis of the mobile entity table received from said at least one other firewall.

13. A method according to claim 12, further **characterized in**

requesting from the at least one other firewall a mobile entity table comprising identifiers of mobile entities which are active in the at least one other firewall.

14. A method according to any one of claims 12 to 13, **characterized in that** the predefined action is an indication of certain time period having elapsed (500) since the first mobile entity table was sent the last time.

15. A method according to any one of claims 12 to 13, **characterized in that** the predefined action is changing (504) the content of the first mobile entity table.

16. A method according to any one of claims 12 to 13, **characterized in that** the predefined action is receiving (506) a request for the first mobile entity table.

17. A firewall (204, 205, 236, 239, 240, 305, 321) **characterized in** comprising

memory and mechanism for maintaining a first mobile entity table comprising identifiers of mobile entities which are active in the firewall,

memory and mechanism maintaining a second mobile entity table comprising identifiers of mobile entities which are active in a predefined set of other firewalls and identifiers of corresponding other firewalls,

mechanism for detecting a new mobile entity, which is not currently active in the firewall,

mechanism for finding on the basis of the second mobile entity table, if the new mobile entity is currently active in another firewall, and

mechanism for querying, from the another firewall, state information related to the new mobile entity, and mechanism and memory for storing the state information in the firewall to be used for processing data packets from/to the new mobile entity, if the mobile entity is currently active in another firewall.

18. A firewall (204, 205, 236, 239, 240, 305, 321) **characterized in** comprising

memory and mechanism for maintaining a first mobile entity table comprising identifiers of mobile entities which are active in the firewall,

mechanism for sending the first mobile entity table to a predefined set of other firewalls as a response to a predefined action,

mechanism for receiving from at least one other firewall a mobile entity table comprising iden-

tifiers of mobile entities which are active in the at least one other firewall, and

memory and mechanism for maintaining a second mobile entity table comprising identifiers of mobile entities which are active in the at least one other firewall and an identifier of the corresponding at least one other firewall on the basis of the mobile entity table received from the at least one other firewall.

19. A computer-readable medium, **characterized in** containing a computer software which, when executed in a computer device, causes the computer device to provide a firewall routine comprising

maintaining a first mobile entity table comprising identifiers of mobile entities which are active in the firewall,

maintaining a second mobile entity table comprising identifiers of mobile entities which are active in a predefined set of other firewalls and identifiers of corresponding other firewalls,

detecting a new mobile entity, which is not currently active in the firewall,

finding on the basis of the second mobile entity table, if the new mobile entity is currently active in another firewall, and

if the mobile entity is currently active in another firewall, querying, from the another firewall, state information related to the new mobile entity, and storing the state information in the firewall to be used for processing data packets from/to the new mobile entity.

20. A computer-readable medium, **characterized in** containing a computer software which, when executed in a computer device, causes the computer device to provide a firewall routine comprising

maintaining a first mobile entity table comprising identifiers of mobile entities which are active in the firewall,

sending the first mobile entity table to a predefined set of other firewalls as a response to a predefined action,

receiving from at least one other firewall a mobile entity table comprising identifiers of mobile entities which are active in the at least one other firewall, and

maintaining a second mobile entity table comprising identifiers of mobile entities which are active in the at least one other firewall and an identifier of the corresponding at least one other firewall on the basis of the mobile entity table received from the at least one other firewall.

21. A computer program comprising program code means for performing all the steps of any of claims 1 to 16 when the program is run on a computer.

10

RULE #	SRC ADDR	DST ADDR	SERVICE	ACTION
1	any	172.16.1.10	http	allow
2	any	any	http	deny
3	10.1.1.0	192.168.1.1	ftp	allow
4	10.1.1.0	any	telnet	allow
5	any	any	any	deny

Fig. 1

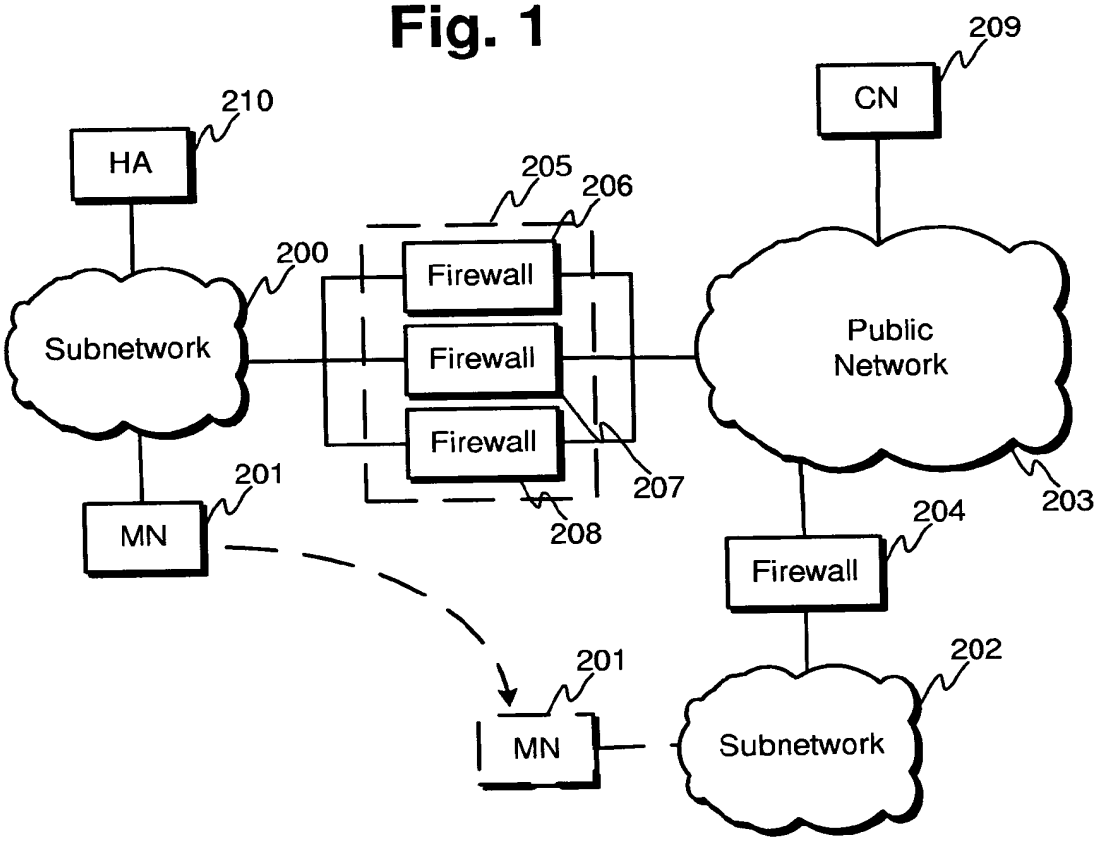

Fig. 2A

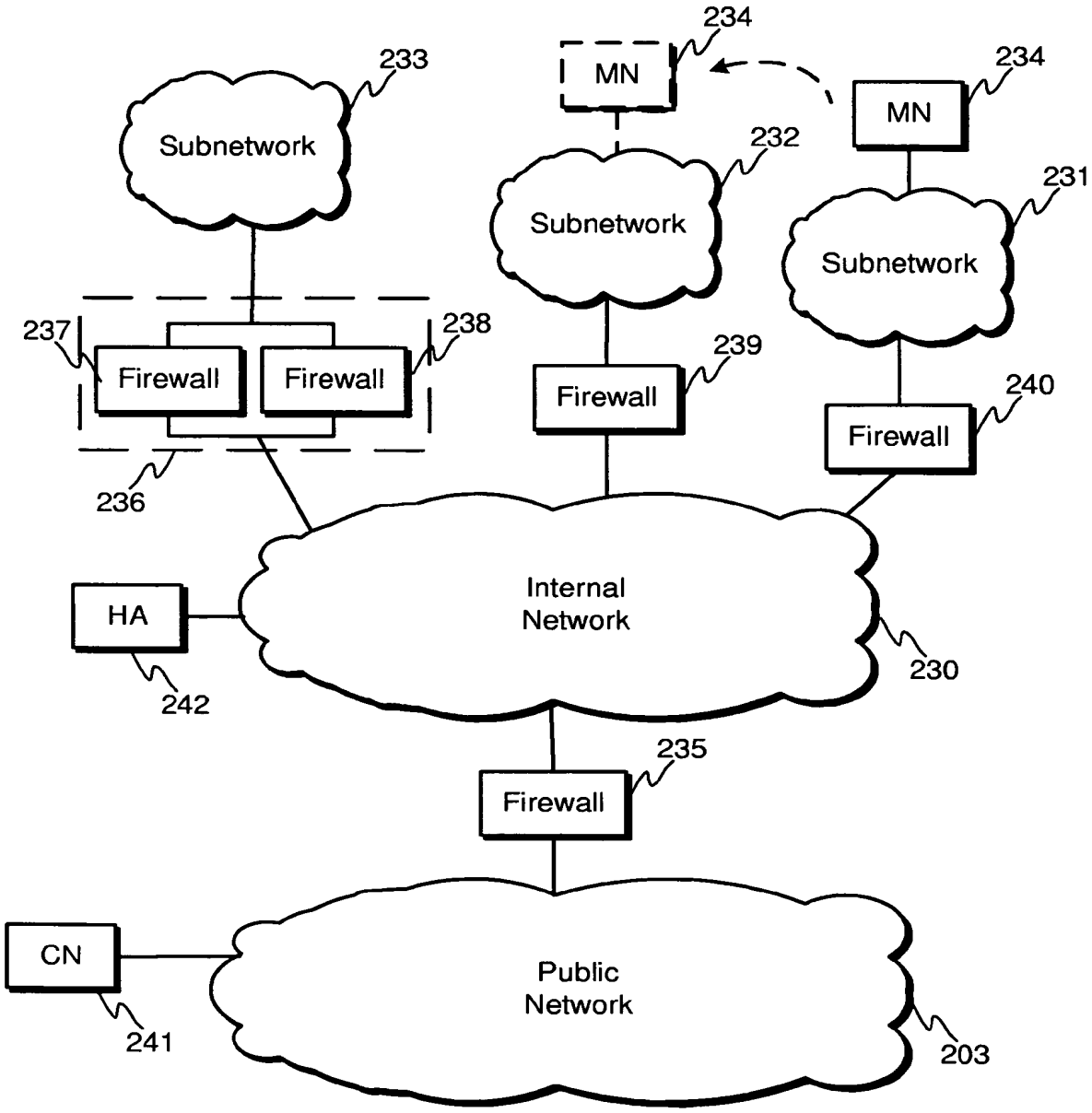

Fig. 2B

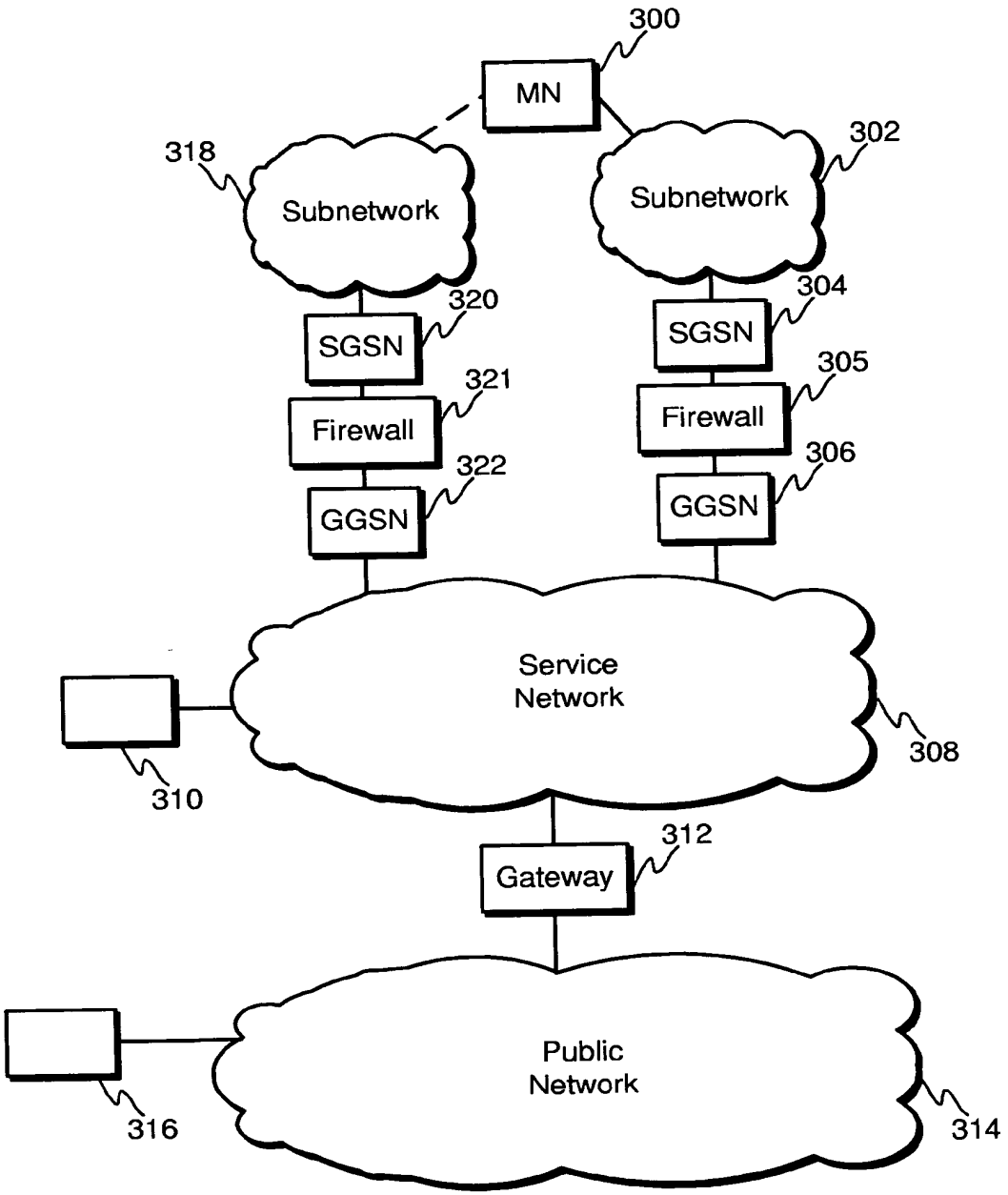

Fig. 3

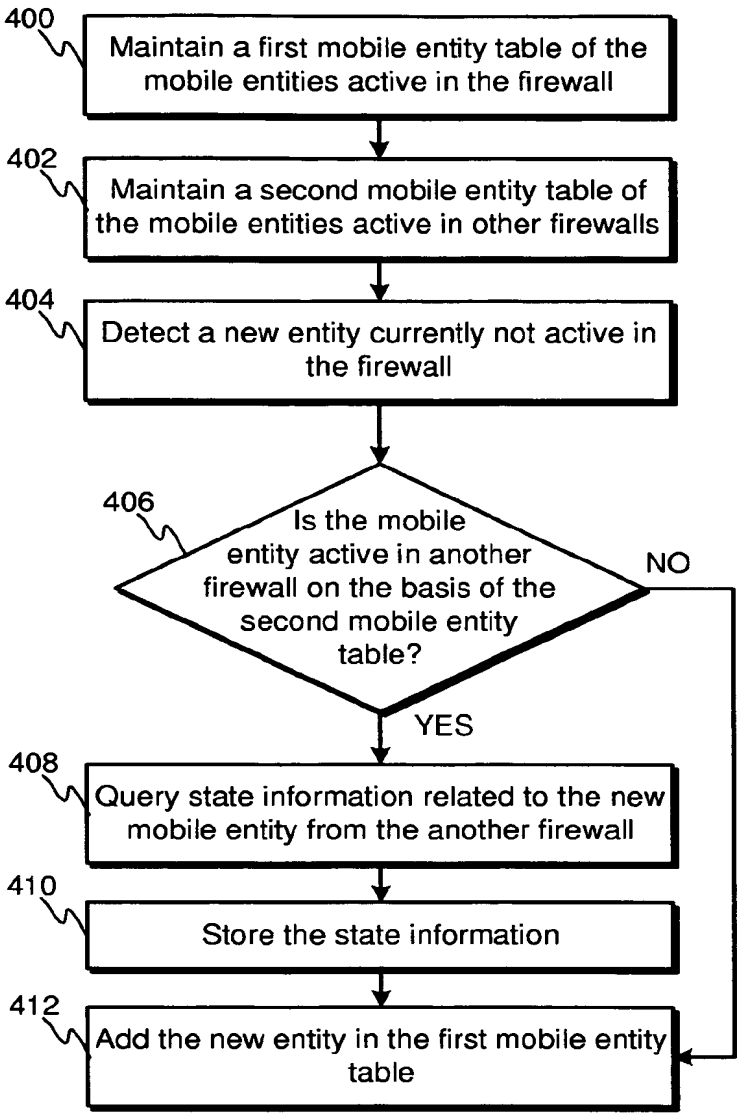

Fig. 4A

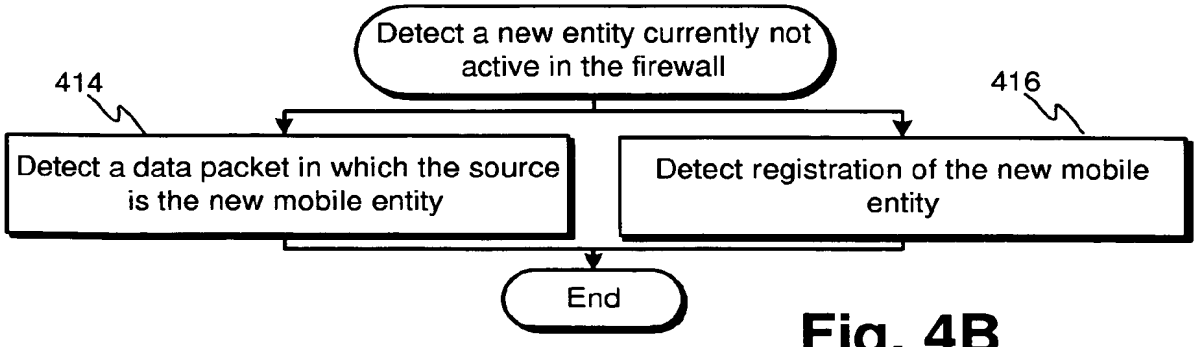

Fig. 4B

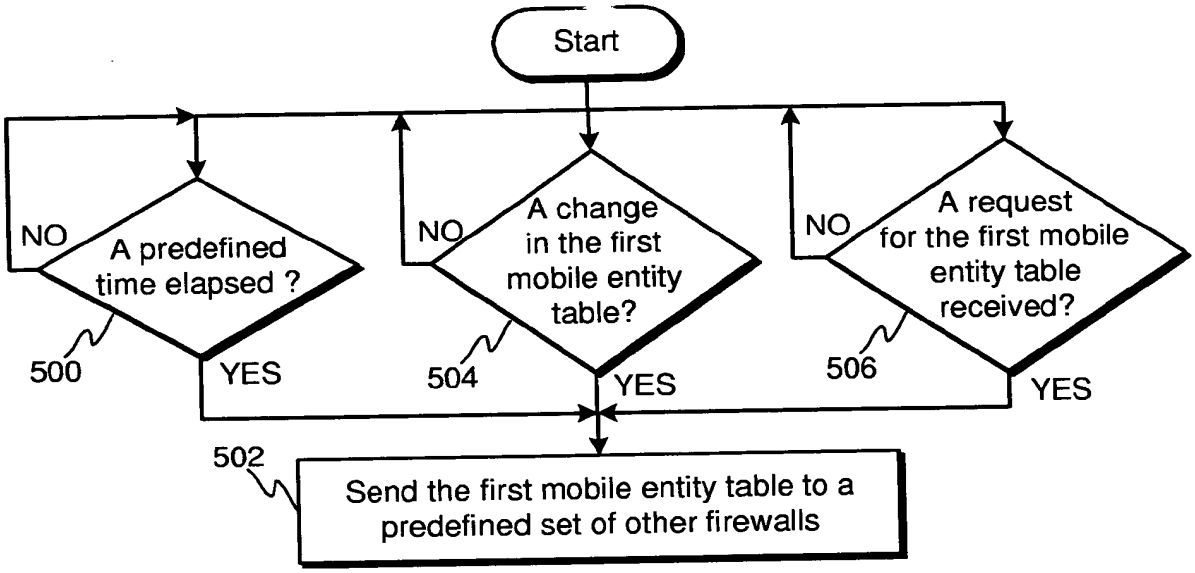

Fig. 5

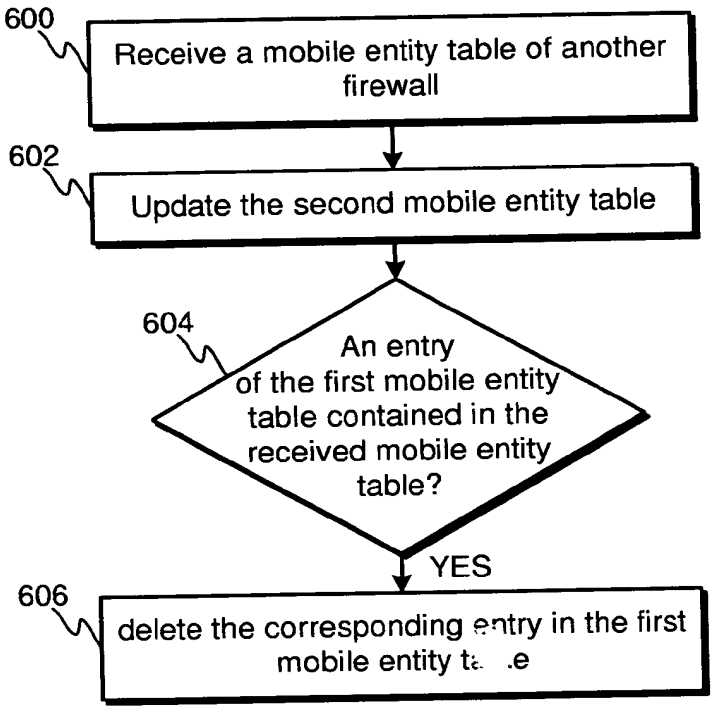

Fig. 6

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 317 112 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
15.12.2004 Bulletin 2004/51

(43) Date of publication A2:
04.06.2003 Bulletin 2003/23

(21) Application number: **02102644.8**

(22) Date of filing: **26.11.2002**

(51) Int Cl.[7]: **H04L 29/06**, H04L 12/56, H04Q 7/38

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **29.11.2001 FI 20012339**

(71) Applicant: **Stonesoft Corporation**
00210 Helsinki (FI)

(72) Inventors:
- **Syvänne, Tuomo**
  01450, Vantaa (FI)
- **Jalava, Mika**
  02580, Siuntio (FI)

(74) Representative: **Äkräs, Tapio**
Kolster Oy Ab,
Iso Roobertinkatu 23,
P.O. Box 148
00120 Helsinki (FI)

(54) Handling connections moving between firewalls

(57) A method of handling mobile entities in a firewall, wherein a first mobile entity table comprising identifiers of mobile entities, which are active in a firewall, and a second mobile entity table comprising identifiers of mobile entities, which are active in a predefined set of other firewalls and identifiers of corresponding other firewalls, are maintained (400, 402) in the firewall. A new mobile entity, which is not currently active in the firewall, is detected (404), after which it is found on the basis of the second mobile entity table, if the new mobile entity is currently active in another firewall. If the mobile entity is currently active in another firewall, state information related to the new mobile entity is queried (408) from the another firewall, and stored (410) in the firewall to be used for processing data packets from/to the new mobile entity.

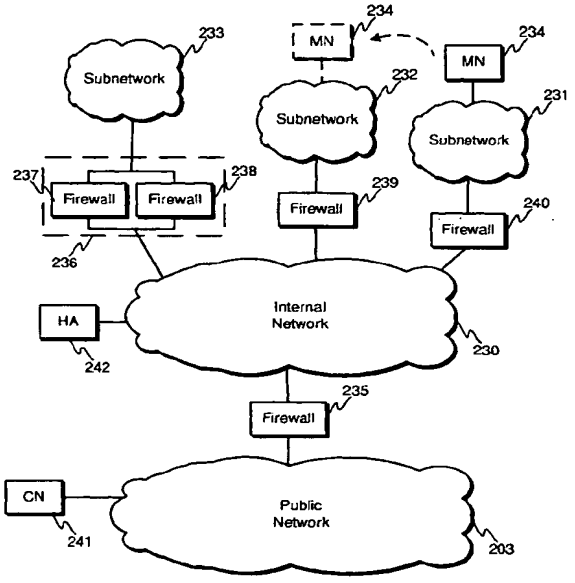

Fig. 2B

EP 1 317 112 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 10 2644

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	US 6 226 523 B1 (KARLSSON TORGNY) 1 May 2001 (2001-05-01) * abstract * * column 4, line 47 - line 51 *	1-21	H04L29/06 H04L12/56 H04Q7/38
A	EP 0 917 320 A (LUCENT TECHNOLOGIES INC) 19 May 1999 (1999-05-19) * abstract * * paragraph [0188] - paragraph [0206] *	1-21	
A	WO 00/52575 A (PACKET TECHNOLOGIES LTD ;DANIELY GAD (IL)) 8 September 2000 (2000-09-08) * abstract *	1-21	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04L
H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	26 October 2004	Bertolissi, E

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 10 2644

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

26-10-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6226523 B1	01-05-2001	AU 765973 B2	09-10-2003
		AU 1989699 A	12-07-1999
		CA 2315208 A1	01-07-1999
		GB 2349779 A ,B	08-11-2000
		JP 2001527356 T	25-12-2001
		WO 9933291 A1	01-07-1999
EP 0917320 A	19-05-1999	US 6400722 B1	04-06-2002
		CA 2249817 A1	14-04-1999
		CA 2249830 A1	14-04-1999
		CA 2249831 A1	14-04-1999
		CA 2249836 A1	14-04-1999
		CA 2249837 A1	14-04-1999
		CA 2249838 A1	14-04-1999
		CA 2249839 A1	14-04-1999
		CA 2249862 A1	14-04-1999
		CA 2249863 A1	14-04-1999
		EP 0912026 A2	28-04-1999
		EP 0910198 A2	21-04-1999
		EP 0917320 A2	19-05-1999
		EP 0917318 A2	19-05-1999
		EP 0912027 A2	28-04-1999
		EP 0912012 A2	28-04-1999
		EP 0917328 A2	19-05-1999
		EP 0918417 A2	26-05-1999
		EP 0912017 A2	28-04-1999
		JP 11289353 A	19-10-1999
		JP 11252183 A	17-09-1999
		JP 11275154 A	08-10-1999
		JP 11275155 A	08-10-1999
		JP 2000022758 A	21-01-2000
		JP 11275156 A	08-10-1999
		JP 11275157 A	08-10-1999
		JP 11284666 A	15-10-1999
		JP 11331276 A	30-11-1999
		US 6665718 B1	16-12-2003
		US 6577643 B1	10-06-2003
		US 6414950 B1	02-07-2002
		US 6421714 B1	16-07-2002
		US 6377982 B1	23-04-2002
		US 6675208 B1	06-01-2004
		US 2002089958 A1	11-07-2002
		US 6393482 B1	21-05-2002
WO 0052575 A	08-09-2000	AU 2570400 A	21-09-2000
		WO 0052575 A1	08-09-2000

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 10 2644

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

26-10-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0052575 A		US 6763469 B1	13-07-2004

EPO FORM P1459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82